

NATIONAL COMPUTER FORENSICS
INSTITUTE REAUTHORIZATION
ACT OF 2022

SPEECH OF

HON. SHEILA JACKSON LEE

OF TEXAS

IN THE HOUSE OF REPRESENTATIVES

Tuesday, June 21, 2022

Ms. JACKSON LEE. Madam Speaker, I stand in support of H.R. 7174, the "National Computer Forensics Institute Reauthorization Act of 2022" which will bolster the education of those defending the American people against cyber security threats.

Soon after the devastating attacks on 9/11, Congress passed the Homeland Security Act of 2002 through which it consolidated the separate branches of our security efforts into one dedicated office.

Through this Act, the Department of Homeland Security provided provisions such as infrastructure protection, chemical, biological, and nuclear defenses, as well as other measures to safeguard national security.

Congress voted in 2012 to reauthorize these important protections. We gather here to do so again today.

During the drafting of the Homeland Security Act of 2002, the United States faced a wave of terrorism and extremism that threatened the lives and liberties of our people.

Today, enemies of the State have evolved to infiltrate our computers, cell phones, and cyber infrastructure.

As a result, companies, organizations, and entire cities are targets for attacks.

Last year, more than 400 U.S. government offices were held ransom or affected by a direct cyber threat.

In 2018, Atlanta, Georgia was nearly crippled by a ransomware attack that wreaked havoc on utilities, parking, and other services in the city. Atlanta taxpayers spent over \$2.6 million in recovery efforts.

Last year, Washington, D.C.'s Metropolitan Police Department was targeted by cyberthugs threatening to publish countless pieces of sensitive data including arrest records, the identities of persons of interest, and even the names of confidential police informants.

In December, a Los Angeles location of Planned Parenthood had the private health information of 400,000 patients stolen through ransomware. Addresses, birthdays, and diagnoses of patients were in the hands of those who meant to do the American people harm.

Ransomware attacks cost federal, state, and local government agencies about \$915 million last year.

Our Nation is vulnerable.

We are at risk.

We must be proactive to protect against larger and more sophisticated attacks.

That is why I stand in support of the "National Computer Forensics Institute Reauthorization Act of 2022" which will continue efforts to train, educate and equip State, local, territorial, and Tribal law enforcement officers to combat cyber-attacks for another 10 years.

With this amended reauthorization, Congress would balance the need for cybersecurity with the prioritization of civil rights, civil liberties, and the safeguarding of private data.

It would also designate curriculum for the Institute, authorize full or partial funding towards attendance at the Institute, require reports of

efficacy, future need, and demographic information, as well as expand on the physical and virtual capacities of the Institute's academic reach.

H.R. 7174 would amend the Homeland Security Act of 2002 to better train those who defend our country from cyber threats today, while preparing for the advanced threats coming tomorrow.

Perhaps the most important section of this Act is the provision outlining the research and development of systems and procedures to enhance the Institute's capabilities and capacity for the future.

If cyber-attackers are willing to target American cities, agencies, and companies today, there is little question that they will be willing to target even more tomorrow.

Our best weapon against such threats is an educated and empowered league of law enforcement and IT professionals working to defend the nation's data, privacy, and security.

Once again, I offer my support for H.R. 7174, "National Computer Forensics Institute Reauthorization Act of 2022" and encourage my colleagues to do the same.

NDO FAIRNESS ACT

SPEECH OF

HON. SHEILA JACKSON LEE

OF TEXAS

IN THE HOUSE OF REPRESENTATIVES

Tuesday, June 21, 2022

Ms. JACKSON LEE. Madam Speaker, I rise in defense of Americans' right to due process in support of the NDO Fairness Act.

This bill amends 18 U.S.C. 2705 to increase the federal regulation of law enforcement's use of non-disclosure orders or "gag orders".

H.R. 7072 requires federal prosecutors to have obtained a written determination from a court proving that their use of a non-disclosure order is necessary.

This bill also would establish a 30-day limit for gag orders, which can be extended for 30 days if deemed necessary.

After the gag-order expires, law enforcement must ensure that the person subject to the gag-order has been notified within 72 hours.

This bill also creates the historic and necessary right for cellular service providers to contest prosecutors' gag orders in court.

Under the status quo, the process for prosecutors to request and be granted access to an individual's personal electronic communication is streamlined, unregulated, and relatively unrestrained.

Prosecutors then petition for a non-disclosure order, stripping the subject's right to know their personal information is being searched.

The NDO also prohibits the subject's ability to block the search of their personal data.

If this intrusion were done in-person—meaning that the government shows up to a person's home, accesses their desktop, secures their personal data, and then refuses to tell that citizen—Americans would be outraged.

The searching of online data is just as egregious a violation of personal privacy.

Establishing transparency within our democracy, especially within our criminal justice system, is necessary to ensure the legitimacy of government and the preservation of our Union.

Just because the ecosystem for data has changed from analog to digital does not give the government the right to full access of whatever information they see as necessary for prosecution.

This legislation tips the scales of justice back toward the American citizen, protecting them from unwarranted, unconstitutional searches of their property.

EXPRESSING THE SENSE OF CONGRESS REGARDING THE EXECUTION-STYLE MURDERS OF UNITED STATES CITIZENS YLLI, AGRON, AND MEHMET BYTYQI IN THE REPUBLIC OF SERBIA IN JULY 1999

SPEECH OF

HON. SHEILA JACKSON LEE

OF TEXAS

IN THE HOUSE OF REPRESENTATIVES

Tuesday, June 21, 2022

Ms. JACKSON LEE. Mr. Speaker, I rise in support of H. Con. Res.E "Expressing the Sense Of Congress Regarding the Execution-Style Murders Of United States Citizens Ylli, Agron, And Mehmet Bytyqi In The Republic Of Serbia In July 1999".

This resolution would demand that the individuals who so unconscionably murdered the Bytyqi Brothers shortly after the end of the Kosovo war be held accountable by the Serbian government.

This resolution reaffirms our commitment to American citizens, that, no matter what, they will receive the justice that they and their families deserve, regardless of how long it has been.

Ylli, Agron, and Mehmet were American citizens traveling on a humanitarian mission to combat the genocide of Serbian Albanians in 1999, who, after unknowingly crossing an unmarked border, were extrajudicially kidnapped, imprisoned, tortured, murdered, and callously thrown into a mass grave by Serbian government officials.

Their bodies were not discovered until 2001.

These officials knew the entire time that the Bytyqi brothers were Americans citizens, and undeterred, carried out crime after crime, even after a Serbian judge ordered the brothers' release.

Despite this horrific crime, despite promises from President Aleksandar Vucic and Foreign Minister Ivica Dacic, not one person has been held responsible in the past 23 years.

We cannot allow this injustice to exist, and we cannot allow other countries to believe that it is in any way acceptable to treat American citizens in this manner.

It is unacceptable that there has been no movement on this case in years.

Ylli, Agron, and Mehmet and the remaining Bytyqi family deserve justice, and the Serbian government agrees. How then has nothing been done to secure this justice?

Since the Serbian government has not acted, the United States must devote resources to fully assist and monitor Serbia's efforts to investigate this crime against American citizens.

No American should experience what the Bytyqi brothers and their families have experienced, and we should make it clear that the United States will always seek justice for its people.

I urge all my colleagues to support H. Con. Res. E “Expressing the Sense of Congress Regarding the Execution-Style Murders of United States Citizens Ylli, Agron, And Mehmet Bytyqi in the Republic of Serbia in July 1999”.

PROMOTING UNITED STATES
INTERNATIONAL LEADERSHIP IN
5G ACT OF 2021

SPEECH OF

HON. SHEILA JACKSON LEE

OF TEXAS

IN THE HOUSE OF REPRESENTATIVES

Tuesday, June 21, 2022

Ms. JACKSON LEE. Mr. Speaker, I rise in support of H.R. 1934, the “Promoting United States International Leadership in 5G Act of 2021”.

H.R. 1934 will enhance the United States’ leadership in setting standards for 5G—or 5th generation—and future evolutions of mobile telecommunications systems and infrastructure.

I would like to thank my colleague, Representative MCCAUL, for introducing this legislation and taking initiative in addressing the rising importance of 5G standards.

Under H.R. 1934, the President will establish an interagency working group consisting of the Secretary of State and the head of each Federal department deemed appropriate.

Within 180 days, the interagency working group will provide a briefing to the House Committee on Foreign Affairs and Senate Committee on Foreign Relations that will include:

A strategy to promote United States leadership in international standards-setting bodies;

A strategy for diplomatic engagement regarding 5G and future generations of mobile telecommunications systems;

A discussion of China’s activity in international standards-setting bodies; and

A strategy regarding private sector communications and stakeholders to propose standards for 5G.

Standards are crucial in the future of telecommunications by allowing for global interoperability.

Global interoperability allows companies to market products around the globe, increase innovation, and benefit from fair competition.

Past generations of wireless technology, 2G and 3G, saw a split between networks used in United States, Europe, and China, which complicated the globalization of the wireless market.

For 5G, standards have converged into primarily one standard.

China has become a leader in setting international standards for 5G. In 2019, China submitted 830 technical documents to the International Telecommunication Union (ITU)—the most of any country.

China’s dominance in 5G standards would give them an advantage in creating chips and software for 5G-compatible phones.

H.R. 1934 addresses this head-on by spearheading American leadership in both 5G standards setting and global cooperation.

Houston was one of the first cities in America to access 5G services with major providers—AT&T, T-Mobile, and Verizon—offering access to Houston customers.

The Texas Comptroller’s Office released a report in 2020 indicating that Houston led 5G growth in Texas.

The adoption of 5G has tremendous potential to create jobs and transform the healthcare, energy, and transportation industries.

CTIA, a trade group for the wireless communications industry, found that 5G could have an economic impact of \$30.3 billion and create 93,700 jobs in Houston.

5G represents the future and will expand technological limits to a new frontier.

It is important that we continue to prioritize the United States’ international leadership as 5G continues to grow.

Mr. Speaker, I urge my colleagues to join me in supporting H.R. 1934.

PREVENT EXPOSURE TO NARCOTICS
AND TOXICS ACT OF 2021

SPEECH OF

HON. SHEILA JACKSON LEE

OF TEXAS

IN THE HOUSE OF REPRESENTATIVES

Tuesday, June 21, 2022

Ms. JACKSON LEE. Madam Speaker, I rise in support of H.R. 5274, known as the PREVENT Act of 2021.

The Prevent Exposure to Narcotics and Toxics Act seeks to amend the Homeland Security Act of 2002 to provide additional training for U.S. Customs and Border Protection personnel.

The training outlined in the amendment would instruct U.S. Customs and Border Protection on containment devices which prevent secondary exposure to fentanyl and other lethal substances.

These containment devices reduce exposure to hazardous substances and can improve investigations by better preserving chemical substances for forensic analysis.

Fentanyl exposure as little as two milligrams can lead to trouble breathing, dizziness and a possible lethal overdose.

CBP (Customer and Border Protection) Officers are at an increased risk of exposure to fentanyl and other lethal substances through inhalation, ingestion, skin contact, etc. This exposure risk was reported by the U.S. Department of Homeland Security’s Office of the Inspector General.

The same report cited that many CBP facilities were ill equipped to store fentanyl and other lethal substances.

These facilities were also not equipped with naloxone, a substance critical in preventing overdose when faced with accidental exposures.

Without proper training on how to contain and prevent these threats, our personnel are at risk of endangering themselves and the people they seek to protect.

It is imperative to defend our law enforcement officers from dangers they face while protecting our communities and Nation. This bill would promote the safety of CBP Officers while promoting the effectiveness of their investigations.

I urge my colleagues to vote in favor of H.R. 5274.

INDUSTRIAL CONTROL SYSTEMS
CYBERSECURITY TRAINING ACT

SPEECH OF

HON. SHEILA JACKSON LEE

OF TEXAS

IN THE HOUSE OF REPRESENTATIVES

Tuesday, June 21, 2022

Ms. JACKSON LEE. Madam Speaker, I rise in strong support of H.R. 7777, the “Industrial Control Systems Cybersecurity Training Act.”

H.R. 7777 amends the Homeland Security Act of 2002 to authorize the Cybersecurity and Infrastructure Security Agency to establish an industrial control systems training initiative that will strengthen the skills of our vital cybersecurity workforce.

Industrial control systems are the devices, systems, networks, and controls used to operate and automate the industrial functions that keep our Nation running.

They are key components in manufacturing, electrical generation, wastewater treatment, and even oil refineries—all of which are necessary for the proper functioning of our country.

While the technological revolution has streamlined many industrial services, it has also left us vulnerable to threats targeting our national utilities and infrastructure.

The “Industrial Control Systems Cybersecurity Training Act” provides an instruction manual for training those on the frontlines of our defense.

First, H.R. 7777 prioritizes increasing access to cybersecurity education courses.

The Act would require the Director to make accessible to the public tuition-free virtual and in-person cyber security courses and trainings for varying skill levels.

It would also ensure that these trainings be available across the country so that those working in even the most remote corners of America have the opportunity to develop their cybersecurity skills.

Trainings would cover topics of cyber defense strategies, the evolution of cyber threats, and strategies for mitigating security vulnerabilities in industrial control systems.

All of these courses would be crafted in collaboration with the National Laboratory of the Department of Energy and when necessary, consultation with expert private sector entities.

Those who wish to harm our country are learning from the best criminals; therefore, we must equally arm our defenders right along side them.

Secondly, H.R. 7777 requires the Director to provide reports on the initiative to the House Committee on Homeland Security and the Senate Committee on Homeland Security and Governmental Affairs.

Through these reports, Congress would not only be able to monitor the quality of courses being offered, but would receive yearly recommendations on how to improve the education and training being offered.

In addition to reporting on the contents of the classes taught, the Director would also be expected to provide information on the race, gender, and regional location of those in attendance.

Through this monitoring process, Congress would be assured not only of current demographic diversity, but also the plans to expand access to industrial control systems cybersecurity training to women and underrepresented populations.